AIATrust
Where smart architects manage risk®

The Threat is Real: Cyber Attacks Against Architectural Firms

*You've built a strong reputation as the architect of choice for an array of clients. Things are going great for your firm…until one day. A client calls to say they were a victim of ransomware. Their investigation traced the source of the initial infection to an email from your firm. Soon, the conversation leads to a potentially very uncomfortable question: "**How does your firm manage cyber risk?"***

Many professional services firms are tempted into believing they're safe from cyberattacks because they don't consider their data to be "sensitive" or desirable information. In reality, they are tempting fate.

Over the past few years, Kroll and Mullen Coughlin have witnessed a sea change in the world of cyber risk. Cybercriminals are sophisticated, deliberate and efficient in how they monetize their efforts. If you use the internet for any reason – even if just for basics such as email, submitting invoices or sharing designs – you are at risk. To a cybercriminal, you can be a primary target, an intermediate conduit to another victim, a cog in a larger attack or scheme, or increasingly, all three.

How does this play out in real-life? In Kroll's investigative work, a common scenario has emerged: A firm is first infected with a banking Trojan after an employee opens a malicious attachment or link in a phishing email message. Actors will search each computer and web browser on your network for Active Directory or finance-related username and password credentials to commit all sorts of financial fraud. Then the finely tuned malware uses email and social engineering to spread from victim to victim. Once the malware runs through its various missions, it deploys ransomware to wring out one last payday.

> *A cybercriminal used a phishing email message sent to one employee of an architectural firm to ultimately gain access to two other accounts. Who were the three targeted individuals? The CEO, secretary for the CFO, and the comptroller.*

From Mullen Coughlin's perspective as counsel, we are cognizant of how regulatory tolerance for data privacy violations continues to harden. State, federal, and international laws are constantly evolving and expanding. Many laws today require that organizations take specific steps if unauthorized access to their information systems occurred, or if covered data was or is reasonably believed to have been subject to unauthorized access or acquisition. Some laws also require covered organizations to take certain steps to:

- assess the cyber security risks of the organization,
- proactively mitigate this risk,
- communicate their information collection and sharing practices, and
- train their staff on information security and incident response.

The inescapable fact is that cyber risk is a problem for every professional services firm. However, while the challenge is complex, a prudent and pragmatic approach is built on common sense principles. A defensible cyber security strategy provides a framework to create a safer, more cyber resilient organization. But in the event of an incident or breach, it also helps you develop a validated, auditable narrative to reply to the question: "*How does your firm manage cyber risk?"*

Cyber Risk Trends

A quick overview of the most recent trends in cyber risk is instructive for any firm that might be harboring a false sense of security that it is at low risk for an attack.

Business email compromise ("BEC") is a major threat that can affect anyone with an email account. According to a Federal Bureau of Investigation ("FBI") alert, from roughly 2013-2018, BEC scams cost victims over $12.5 billion. The FBI also noted that every U.S. state had victims.

> *A large architectural firm noticed an increase in account receivables and in particular, one organization that had failed to pay previous invoices totaling $500,000. These invoices were sent on a monthly basis via email from one firm employee. This firm employee called her contact at the organization, and her contact reported that they had, indeed, wired money to pay these invoices. The contact reported that the money was wired to the new bank account reported to it by the firm employee. The firm employee was confused as the firm's bank account had not changed.*
>
> *Further investigation revealed that she had fallen victim to a phishing scam. An unauthorized individual gained access to her email account and sent revised invoices to her contact with wiring instructions for an account in China that did not belong to the firm. The actor had also created rules to forward to a separate email folder all emails sent by this organization to her; in this way, the firm employee would not be able to easily see evidence of the intruder impersonating her. Neither the firm nor its client was able to recover the monies, and the firm made a business decision to not seek repayment of the funds in order to maintain the business relationship.*
>
> *Additional investigation revealed that the employee had stored in her email account the names and Social Security numbers of the firm's employees and, because the firm was unable to rule out unauthorized access by the intruder to this*

information, the firm was required to disclose the incident to its staff, state regulators, and consumer reporting agencies

The Emotet banking Trojan is particularly successful in carrying out BEC schemes because its creators gave it the capability to spoof a victim's legitimate email address ***and*** build on existing conversation threads that it steals and exfiltrates from infected computers. This combination results in well-disguised emails that avoid the "stranger danger" red flag. Kroll has found them to be very successful in getting opened by recipients while also breezing past antivirus filters. So while a cyberattacker may have low expectations on monetizing their attack on you, they could very well be playing a long game to get to one of your clients.

Ransomware attacks have also been on the rise in 2019. Every business is a target, and the ones with lax security, misconfigured applications, or unpatched systems play right into a hacker's hands.

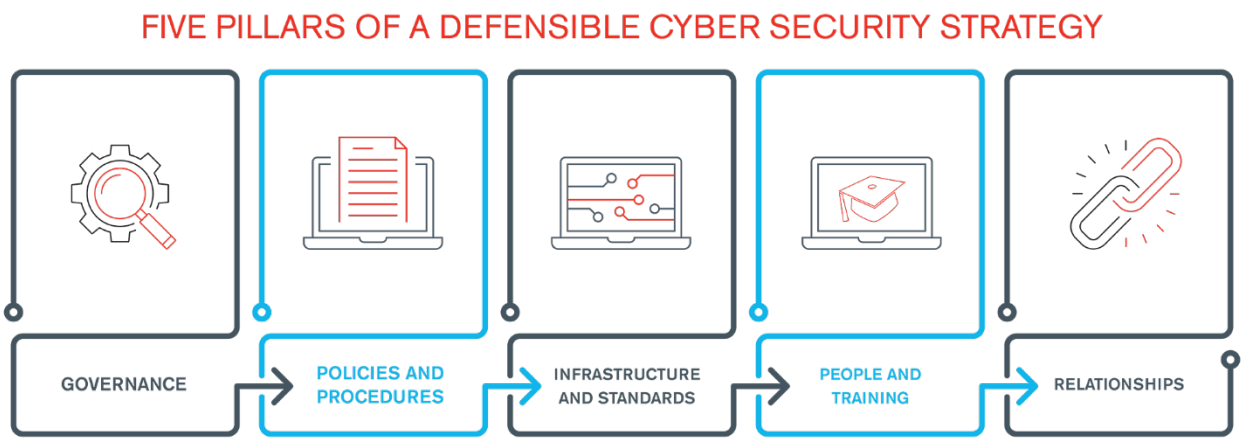
A mid-sized, full-service architectural firm based in the United States became a victim of ransomware that prevented employees from accessing any of their files. An investigation revealed that several malware variants had gotten past the firm's antivirus solution, leading up to the ultimate encryption of several servers. Actors associated with these types of attacks are typically interested in revenue accumulation through ransom payments and not by collecting sensitive data.

Managed service providers have been particularly targeted this year to spread ransomware to their clients. Even the most nominal ransoms are pure profit. And the costs aren't limited to paying a ransom. There are the costs associated with lost productivity and billable hours, delayed projects, IT forensics and fixes, and reputational headaches, not to mention the possibility of regulatory action.

Several small architectural firms relied on an external IT firm to support its information systems. The external IT firm could remotely access the firms' information systems to quickly troubleshoot issues. This IT firm supported a network of small architectural firms, utilized the same remote access tool to do so, and used the same credentials to access each network. The external IT firm experienced a network intrusion, and the attackers utilized the remote access tool and common credentials to introduce ransomware to each small architectural firms' information systems. This resulted in the firms being unable to access their information systems, including plans needed to support customer projects, resulting in a delay in performance. The information systems remained non-operational for two weeks before they could be restored to functionality.

Five pillars of defensible cyber security

A defensible cyber security strategy is built on five pillars:



Jason Smolanoff, Kroll's Global Leader for Cyber Risk, has written that a well-executed defensible cyber security strategy will enable a company to respond more confidently in the event of a cyber event with a documented narrative of its having followed a range of best practices, such as the following:

> "We as a company performed a threat-based assessment and we did this based upon the type of data we have, the business we're in, and the kind of data we're storing and transacting. And, we've taken reasonable measures to protect our data from the threats that we think are most prevalent to us. And if an attacker does get into our network, they must have taken some extraordinary measures to bypass our reasonable security."

Governance

Leaders should strive to foster a strong cyber security culture throughout all their operations, where employees and third parties are continually thinking about the cyber security implications of what they do on a daily basis. Leaders themselves should model good cyber security practices and invest in people with requisite cyber security skills and in appropriate types of technology to aid them.

Policies and Procedures | Infrastructure and Standards

Your information security strategy should work effectively in your current day-to-day operations, but also account for the dynamic nature of business and laws applicable to the

organization. Cyber security policies and procedures[i] often overlap with and are driven by best practice standards, such as the **NIST Cyber security Framework** and the **Center for Internet Security ("CIS") Controls**. Whichever framework you choose, be aware that monitoring and testing compliance with policies and procedures is key.

These standards also cover the role of technology in cyber defense. A risk assessment performed by an independent cyber security professional can be an eye-opener as to whether or not you are protecting the right assets in the best way.

People and Training

Training and cyber security awareness programs that are relevant to real-life decision-making are critical. Consider supplementing annual cyber security training with periodic updates on any recent threats your firm has experienced, or new scams reported by law enforcement or industry resources (such as the AIA Trust).

Training staff on your incident response plan should be a priority. We also recommend that firms run a tabletop exercise at least once a year (quarterly is better for larger organizations) to test this plan and uncover any gaps between policy and real-life action. Likewise, IT staff should be tested and trained on how to respond in the face of a potential intrusion or attack. Human nature being what it is, many IT teams will first try to fix an issue themselves. Having a pre-established escalation process for threat response can potentially save significant time and money.

Relationships

For many firms, cyber security is not a core strength or area of expertise. Prior to an actual incident occurring, an organization should understand what coverage is afforded under its cyber insurance policies and requirements for such coverage to be provided, and also form relationships with the legal counsel and other service providers that may play a critical role in investigating and responding to an incident.

Recommendations from the Front Lines

Kroll investigates over 1,500 cyber matters annually for clients around the world. Based on this experience, we recommend that organizations prioritize the following practices to more effectively protect their data and the bottom line:

- Transfer risk via **cyber insurance** coverage.
- Implement **multifactor authentication** (2FA or MFA) for any and all access to company network resources, with a particular focus on remote access.
- Ensure your **antivirus program is up-to-date** and **deploy an endpoint threat monitoring tool** to aid in detecting today's polymorphic malware (i.e., malware that is able to change its characteristics and thereby evade traditional antivirus programs).

- Assess **vendor reliance and connectivity** to your information and information systems and assess the risk posed to your organization via this reliance. As part of this assessment, ensure vendors maintain appropriate cyber liability insurance and are contractually obligated to report to you instances of suspected or confirmed compromises in the security of your information and information systems.
- Understand **legal and contractual obligations** your organization may have should unauthorized access to your information systems or your data occur.

Finally, be sure to regularly and completely document all the "due care" measures you have taken. This will comprise your defensible cyber security narrative should a breach occur.

Cyber resiliency a journey

By now, you can see that as an architectural firm, you are as likely a target for cyberattackers as any enterprise in any business sector. Just because you don't regularly work with the kind of data that makes news headlines doesn't mean your data isn't valuable to someone. In fact, building plans, infrastructure schematics, and knowing how and where all the "smart" components are built into today's structures may prove especially attractive to someone bent on monetizing that knowledge. Beyond that, you have seen how cyberattackers can use your digital connections as a springboard into a client's environment.

Many professional services firms, especially those in the earliest stages of cyber maturity, can benefit from a more in-depth understanding of real-world threat and challenges. The following five articles collectively provide a wide-ranging view of the current cyber threat landscape:

- Cyber Incident Actors: Who Are They?
- Insider Actors
- Cyber Incident Methods
- The Life Cycle of an Attack
- Monitoring the Threat Environment

Cyber resiliency is a journey, not a race toward an imaginary finish line. What you gain with maturity is not only a better understanding of the risks you face, but also greater insight into how to defend and protect what you work so hard to build every day.

---

[i] *For more information on core policies that should be part of a defensible information security strategy, see "9 policies and procedures you need to know about if you're starting a new security program", Gary Hayslip, CSO Online.*